

CLAIMS

1 1. Method for the secure execution of an instruction sequence of a
2 computer application in the form of typed data stored in a first series of given
3 locations in a memory of a computer system, particularly an embedded microchip
4 system, characterized in that additional data called type information elements are
5 associated with each of said typed data, in order to specify the type of these data, in
6 that said type information elements are stored in a second series of given storage
7 locations (4, 5) in said memory (1) of a computer system (8), and in that before the
8 execution of instructions of a predetermined type, a continuous verification is
9 performed, prior to the execution of predetermined instructions, of the matching
10 between a type indicated by these instructions and an expected type indicated by said
11 type information elements stored in said second series of storage locations (4, 5), so
12 that said execution is authorized only when there is match between said types.

1 2. Method according to claim 1, characterized in that each of said type
2 information elements is constituted by a string of bits stored in storage locations of
3 said second series (4, 5) that correspond one-to-one with storage locations in said first
4 series (2, 3) in which said associated typed data are stored, and the configuration
5 whereof represents one of said types of typed data.

1 3. Method according to claim 1, characterized in that, said instructions
2 being those of an application written in "Java" (registered trademark) language, said
3 typed data are constituted by typed objects, in that said computer system incorporates
4 a piece of software called a "Java" virtual machine (5) that manipulates said typed
5 objects, in that said storage locations (2-5) in said memory (1) of the computer system
6 (8) being organized into stacks comprising a given maximum number of levels, each
7 level constituting one of said storage locations, said typed objects are stored in at least
8 a first elementary stack called a data area (2) and a second elementary stack called a
9 local variable area (3), and in that said type information elements are distributed into
10 two additional elementary stacks (4, 5) that correspond one-to-one with said first (2)

4 constituting one of said storage locations, said typed data are stored in at least a first
 5 elementary stack called a data area (2) and a second elementary stack called a local
 6 variable area (3), and in that said second series of storage locations is also organized
 7 into elementary stacks (4, 5) that correspond one-to-one with said first (2) and second
 8 (3) elementary stacks.

1 9. System according to claim 8, characterized in that said type information
 2 elements stored in said second series of storage locations (4, 5) are associated with
 3 additional information elements that determine the size of said storage locations in
 4 said stacks (2, 3) storing said typed data.

1 10. System according to claim 7, characterized in that said embedded
 2 system is a smart card (8).

10031226-011702